Pourquoi la négociation de TLS de l'ESA à un serveur cible échoue-t-elle en dépit de STARTTLS étant disponible ?

Contenu

[Introduction](#)
[Informations générales](#)
[Pourquoi la négociation de TLS de l'ESA à un serveur cible échoue-t-elle en dépit de STARTTLS étant disponible ?](#)
[Informations connexes](#)

Introduction

Ce document décrit comment identifier la panne de négociation de Layer Security de transfert (TLS) quand **STARTTLS est disponible dans les commandes de Protocole SMTP (Simple Mail Transfer Protocol) EHLO et le serveur ne se conforme pas à RFC1869.**

Informations générales

Le TLS est activé sur l'appliance de sécurité du courrier électronique (ESA) avec un certificat valide. Le TLS est activé sur le serveur cible et STARTTLS est vu quand une connexion de SMTP est établie.

Pourquoi la négociation de TLS de l'ESA à un serveur cible échoue-t-elle en dépit de STARTTLS étant disponible ?

Les essais ESA à connecter au serveur cible à l'utilisation du TLS, cependant, négociation de TLS échoue avec cette erreur sur les **mail_logs de l'**ESA**/cheminement de message**.

```
Info: DCID xxxxxx STARTTLS command not supported.
```

Selon RFC1869, la première réponse à **EHLO** devrait être ehlo-**correcte-rsp** et ehlo-**correct-rsp** a ces syntaxe et commande :

```
Info: DCID xxxxxx STARTTLS command not supported.
```

Exemple incorrect de conversation de SMTP de syntaxe RFC

```
Info: DCID xxxxxx STARTTLS command not supported.
```

Il signifie que tout là est avant l'ehlo-**line** (250-mail.domain1.com, dans cet exemple) est considéré comme message d'accueil. Ainsi, l'ESA ne considèrera pas la commande **250-STARTTLS**

disponible et signalera la **commande STARTTLS non prise en charge**. Référez-vous à https://tools.ietf.org/html/rfc1869 pour plus de détails.

Exemple correct de conversation de SMTP de syntaxe RFC

```
220 mail-esa.com ESMTP
EHLO connecting.server.com
250-mail-esa.com <--- This is the 250 destination server greeting.
250-8BITMIME
250-SIZE 33554432
250 STARTTLS <--- STARTTLS is available after the greeting, it's not considered a greeting as
per RFC.
```

Informations connexes

- Documentation RFC 1869
- Guide complet de TLS ESA
- Support et documentation techniques - Cisco Systems